Unified Information Security Framework

A Collaborative Approach to Developing Security Standards and Guidelines

U.S.- India Standards in Trade Workshop

September 15, 2014

Dr. Ron Ross

Computer Security Division

Information Technology Laboratory



Advanced

Advanced Persistent Threat

An adversary that —

- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations:
 - To exfiltrate information;
 - To undermine / impede critical aspects of a mission, program, or organization; and
 - To position itself to carry out these objectives in the future.



Classes of Vulnerabilities

A 2013 Defense Science Board Report described—

- Tier 1: Known vulnerabilities.
- Tier 2: Unknown vulnerabilities (zero-day exploits).
- Tier 3: Adversary-created vulnerabilities (APT).





Unified Information Security Framework

NIST Special Publication 800-39
 Managing Information Security Risk:
 Organization, Mission, and Information System View

NIST Special Publication 800-30
 Guide for Conducting Risk Assessments

NIST Special Publication 800-37
 Applying the Risk Management Framework to Federal Information Systems

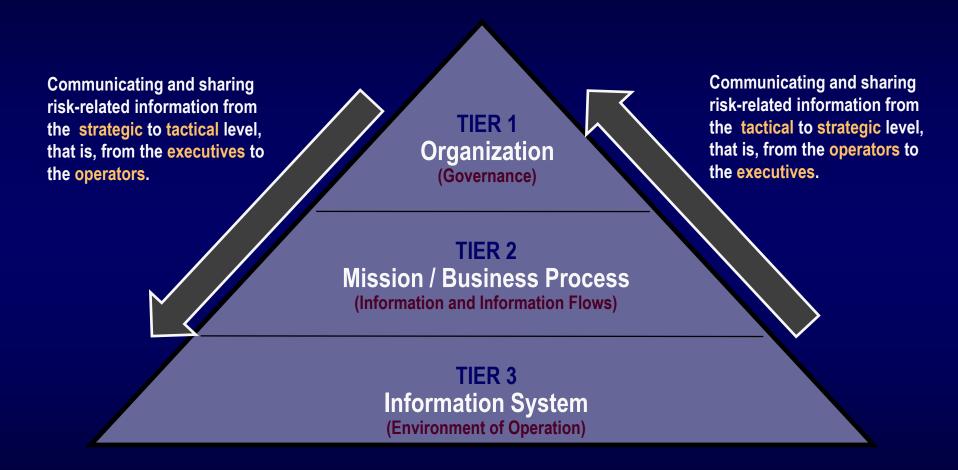
NIST Special Publication 800-53
 Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53A
 Guide for Assessing the Security Controls
 in Federal Information Systems and Organizations





Institutionalizing Risk-Based Security





Risk Management Framework

Starting Point

CATEGORIZE



MONITOR Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.



Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

Security Life Cycle



SELECTSecurity Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.



AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.



ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

IMPLEMENTSecurity Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.









Contact Information

100 Bureau Drive Mailstop 8930 Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross (301) 975-5390 ron.ross@nist.gov

Administrative Support

Peggy Himes (301) 975-2489

peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Pat Toth (301) 975-5140 patricia.toth@nist.gov

Arnold Johnson (301) 975-3247

arnold.johnson@nist.gov

Kelley Dempsey (301) 975-2827

kelley.dempsey@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov

